

10/18/99

JCSB/05

U.S. Department of Commerce
Patent and Trademark Office
PATENT

A

UTILITY PATENT APPLICATION TRANSMITTAL

Assistant Commissioner for Patents
Washington, D.C. 20231
BOX PATENT APPLICATIONAttorney Docket No.: PA990566
Date: October 18, 1999
Express Mail Label No.: EJ824857695USJCSB/05
09/419968
10/18/99

Dear Sir:

Transmitted herewith for filing is the patent application of:

Inventor(s): Sandip SarkarFor: Random Number Generation for Encrypting Cellular Communications

Enclosed are:

1. ☒ Patent application (12) total pages.
2. ☒ Drawings: ☒ Formal (5) sheet(s) or ☐ Informal () sheet(s).
3. ☒ Declaration/Power of Attorney: ☐ Signed ☒ Unsigned
4. ☐ An Assignment () pages and Recordation Form Cover Sheet.
5. ☐ A Preliminary Amendment () pages.
6. ☐ Information Disclosure Statement (IDS):
 - a. ☐ PTO-1449
 - b. ☐ Copies of IDS Citations (number of citations:)
7. ☐ Other:

CLAIMS:	(a) Filed	(b) Extra Claims	Large Entity Fee	Fee Paid
Total*	8 - 20	0	x \$18 =	\$0.00
Independent**	2 - 3	0	x \$78 =	\$0.00
Multiple Dependent Claim(s): <input type="checkbox"/> No <input type="checkbox"/> Yes			\$260	\$
APPLICATION FILING FEE			\$760	\$760.00
*If the number in column a is less than 20, enter 0 in column b. **If the number in column b is less than 3, enter 0 in column b.			TOTAL FEE	\$760.00

8. ☐ A check in the amount of \$_____ is enclosed to pay the filing fee.
9. ☒ Please charge Deposit Account No. 17-0026 of QUALCOMM Incorporated the amount of \$760.00. The Commissioner is hereby authorized to charge payment of any additional fees which may be required, or credit any overpayment, to said Deposit Account No. 17-0026. A duplicate of this sheet is enclosed for fee processing.
10. ☒ The Commissioner is further hereby authorized to charge to said Deposit Account No. 17-0026, pursuant to 37 CFR 1.25(b), any fee whatsoever which may become properly due or payable, as set forth in 37 CFR 1.16 to 37 CFR 1.18 inclusive, for the entire pendency of this application without specific additional authorization.

Date: October 18, 1999Signature: Sean English

Sean English, Reg. No. 37,319

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-4828
Facsimile: (858) 658-2502

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of)
Sandip Sarkar) For: Random Number Generation for
Serial No. Unknown) Encrypting Cellular Communications
Filed: Herewith) Group Art Unit: Unknown

CERTIFICATE OF MAILING UNDER 37 CFR § 1.10

Asst. Commissioner of Patents
BOX PATENT APPLICATIONS
Washington, D.C. 20231

Dear Sir:

"Express Mail" mailing label No. EJ824857695US
Date of Deposit OCTOBER 18, 1999

I hereby certify that the following papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above and is addressed to the Asst. Commissioner of Patents, Box Patent Applications, Washington, D.C. 20231:

PATENT APPLICATION IN 12 PAGES; TRANSMITTAL LETTER IN DUPLICATE; FIVE SHEETS OF FORMAL DRAWINGS; UNSIGNED DECLARATION/POWER OF ATTORNEY; AND POSTCARD

Kayla R. Seignious

(Name)


(Signature)

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 845-3313
Facsimile: (858) 658-2502

RANDOM NUMBER GENERATION FOR ENCRYPTING CELLULAR COMMUNICATIONS

BACKGROUND OF THE INVENTION

5

I. Field of the Invention

The current invention relates to wireless communications networks. More specifically, the present invention relates to a novel and improved method of generating random data for the purpose of encrypting transmissions
10 in wireless communications systems.

II. Description of the Related Art

Encryption schemes for wireless communications require continuous
15 pools of random data. There are a number of ways to generate bits with good spectral properties through software. However, any software produced random number must be pseudo-random by its very nature rather than truly random, as all number sequences generated by software are periodic. Such psuedo-random sequences are susceptible to being deciphered by a third party.
20 Only hardware generated data can be mathematically random. Although other techniques such as employing the voltage jitter from key presses or the time delay between key presses are known, the present invention has significant advantages over these techniques which are either pseudo-random or do not supply continuous random data.

25 Presently, there is no ideal method of continuously generating a sufficient supply of truly random data from existing wireless phone hardware for encrypting wireless communications.

SUMMARY OF THE INVENTION

The present invention is a novel and improved method for generating a continuous pool of random data bits for wireless communications encryption by employing hardware that is already available in conventional wireless phones. In particular, the present invention uses the random nature of the propagation path and the receiver front end, and their effect on the received signal characteristics, to generate a set of random numbers. The present invention is described in terms of a CDMA wireless phone, but the principles are readily adapted to other wireless modulation techniques.

BRIEF DESCRIPTION OF THE DRAWINGS

The features, objects, and advantages of the present invention will become more apparent from the detailed description set forth below when taken in conjunction with the drawings in which like reference characters identify correspondingly throughout and wherein:

FIG. 1 is a high level flowchart diagram of the random data collection method of the present invention.

FIG. 2 is a simplified diagram of a partial CDMA phone signal path through CDMA hardware apparatus.

FIG. 3 is an apparatus diagram of a Receive Automatic Gain Control Circuit.

FIG. 4. is an apparatus diagram of an I/Q DC Offset Correction Loop.

FIG. 5 is an apparatus diagram of a Time Tracking Loop.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

FIG. 1 shows a high level overview of the exemplary method for generating a pool of random data, often required for encryption, from common CDMA phone hardware. The method is readily amended by omission or re-ordering of the steps illustrated and without departing from the scope of the present invention. The present invention is described in the context of CDMA phones. However, the present invention will be equally applicable to other modulation techniques.

In current CDMA systems, data is transmitted in 20 millisecond frames. The method of the present invention is capable of producing four random data bits for each frame, equal to 20 milliseconds, using CDMA variables available during a normal phone call. The invention generates the data from truly random sources present in the received signal. These generated random data bits are collected in a random data pool and made available to encryption processes.

In block **100**, in the exemplary embodiment, the Receive Automatic Gain Control (AGC) circuit of the CDMA phone is employed to generate two random bits of data every 20 milliseconds. Generation of random bits from the Receive AGC circuit is described in detail in FIG 3. The Automatic Gain Control element is employed in wireless phones to keep the in-band energy presented to the demodulator at a fixed level. The received in-band energy fades in a random fashion due to changes in the propagation path from shadowing, fading and multi-path phenomenon. The received signal is normalized by means of a variable gain amplifier of the AGC to provide a first set of random bits. Because the gain of the variable gain amplifier varies continuously, one skilled in the art will understand that the random variable may be extracted at an arbitrary rate from the AGC. Moreover, more or less than two bits may be extracted in the random number generator.

In block **102**, in the exemplary embodiment, the In Phase (I)/Quadrature Phase(Q) DC Offset Correction Loop of the CDMA phone is employed to generate one random data bit every 20 milliseconds. Generation of random bits from the DC Offset Correction Loop is described in detail in FIG 4. The DC
5 Offset Correction Loop element is employed in wireless phones to correct a small DC offset introduced to the received signal during analog to digital conversion **206**. The DC offset is added to the digital signal in a random fashion due to effects of the conversion process on analog signal characteristics. The DC Offset Correction Loop normalizes the mean DC value of the converted
10 signal to zero by means of gain amplification and summing, to provide an additional random bit. Because the DC offset varies continuously, one skilled in the art will understand that the random variable may be extracted at an arbitrary rate from the DC Offset Correction Loop. Moreover, more or less than one bit may be extracted in the random number generator.

15 In block **104**, in the exemplary embodiment, the Time Tracking Loop of the CDMA phone is employed to generate one random bit every 20 milliseconds. Generation of random bits from the Time Tracking Loop is described in detail in FIG 5. The Time Tracking Loop element is employed in wireless phones to maintain bit synchronization regardless of fluctuations in
20 propagation path delays. Propagation path delays vary in a random fashion due to changes in the propagation path from shadowing, fading and multi-path phenomenon. The Time Tracking Loop samples and adjusts the received signal by means of summing and scaling, to provide an additional random bit. Because the propagation path delay varies randomly, one skilled in the art will
25 understand that the random variable may be extracted at an arbitrary rate from the Time Tracking Loop. Moreover, more or less than one bit may be extracted in the random number generator.

Through novel use of the Receive AGC circuit, In Phase/Quadrature (I/Q) DC Offset Correction Loop, and Time Tracking Loop, the exemplary
30 embodiment of the present invention produces 4 bits of random data per frame interval during phone use. Because the data is generated with hardware, it is truly random, rather than software generated data, which must be pseudo-

random by nature. Such sequences of pseudo-random data are highly susceptible to being deciphered by a third party, while random data produced by the present invention is not.

FIG. 2 illustrates a simplified partial signal path within common CDMA phone receive hardware apparatus. **FIG. 2** shows the path of the signal only through the hardware used by the invention to generate random data.

Antenna **202** is a transducer that converts RF (radio-frequency) fields into (alternating current) AC or vice-versa. A receive antenna intercepts RF energy and delivers AC to electronic equipment. The received analog signal reaches antenna element **202**, and is downconverted to a baseband analog signal by the receive demodulator element **204**. After downconversion, the signal passes to an Analog to Digital Converter element **206**.

The Analog to Digital Converter circuit element **206** converts the demodulated analog signal to a digital signal, and performs additional signal processing. During analog to digital conversion, a small Direct Current (DC) offset is introduced into the signal. After the signal is converted, the digitized signal passes simultaneously to the Receive AGC circuit element **208**, the DC Offset Correction Loop element **210**, and the Time Tracking Loop element **212** within the phone where random bits of data are generated each time a frame of data is received. Each newly generated bit of random data is input to Random Number Selector Subsystem element **214**.

Random Number Selector Subsystem **214** is comprised of digital shift registers which generate a new random number each time they are fed with new random bits and shifted. In the exemplary embodiment, the action of feeding and shifting occurs every 20 milliseconds. It will be understood by one skilled in the art that the principles described can be used to provide random bits at other time intervals. A new random number is supplied to Encryptor element **218** every 20 milliseconds.

Normal unencrypted wireless transmission data is readied for encryption by Data Generator element **216**. Normal transmission data may include digitized voice or other communications data. The unencrypted data generated by Data Generator element **216** passes to Encryptor element **218**.

Encryptor element **218** employs data encryption processes which use the pool of random numbers produced by Random Number Selector Subsystem **214** to encrypt the normal data. The encrypted data output of Encryptor **218** passes to Transmitter element **220**.

5 Transmitter element **220** modulates the encrypted signal and processes it for transmission by the transmit antenna element **222**.

Element **222** is the apparatus transmit antenna. Transmit antenna element **222** is fed with the modulated encrypted signal and generates an RF field.

10 **FIG. 3** illustrates the apparatus employed in the exemplary embodiment of the present invention to generate 2 random bits of data from the demodulated digital receive signal input to the Receive AGC **208** every 20 milliseconds. Element **302** illustrates the received I/Q data input path passing to the AGC circuit. I/Q data refers to the In phase and Quadrature phase data
 15 samples produced by Quadrature Phase Shift Keying (QPSK) demodulation. The AGC circuit functions to provide a constant energy signal for demodulation. In so doing, AGC **208** produces a random variable intermediate output, known as the Receive AGC Adjusted bits (RX AGC ADJ) **310**, from the raw chip level input I/Q samples **302**. In CDMA technology, time is often
 20 measured in units of chip. Where CDMA frequency is 1.2288MHz, 1 chip = $1/(1.2288\text{MHz}) = 813.8$ nanoseconds.

In gain stage element **304**, the received signal is multiplied by a gain value. The gain value varies depending on parameters of the wireless phone hardware. Gain values vary in accordance with internal number
 25 representations of hardware components. The range of numbers represented within a component is determined by the number of bits allocated to represent the value. For example, the range of a component 4 bit number may be -7 to 7, while the range of an 8 bit microprocessor would be -128 to 128. If the range of the component values does not match the range of wireless phone controlling
 30 microprocessor devices, the values are scaled up or down in order to use the full value range of the controlling microprocessor, so that information is not lost.

Summer element **306**, sums the I/Q sample with previous samples, every 20 milliseconds. The signal is passed to Low Noise Amplifier (LNA) and Receive Linearizer element **308**, which in the exemplary embodiment produces 8 RX AGC ADJ bits every 20 milliseconds. Element **308** also linearizes the
 5 signal for input to Pulse Density Modulator (PDM) element **312**.

PDM **312** converts the digital signal to analog for use by other CDMA hardware not involved in random number generation.

The two least significant bits (LSB) of RX_AGC_ADJ dither in a manner corresponding to the instantaneous variations of white noise in the received
 10 signal. It can be shown that these two bits are mathematically random because they are derived from mathematically random white noise.

The random bits generated by the Receive AGC are fed to the Random Number Selector Subsystem **214**.

FIG. 4 illustrates the apparatus employed by the exemplary embodiment
 15 of the present invention to generate 1 random bit of data from the demodulated digital receive signal input to the DC Offset Correction Loop every 20 milliseconds. The DC Offset Correction Loop functions to correct for I/Q offset introduced by the analog to digital conversion process. After the input signal passes through the DC Offset Correction Loop, the I/Q offset has a mean value
 20 of zero.

RX DATA, element **404** inputs the received I/Q data to DC Offset Correction Loop **210**.

Receive spectral inversion bit generator **402** provides the receive spectral inversion bit input to DC Offset Correction Loop **210**. The spectral
 25 inversion bit takes a value of 1 or 0. The spectral inversion bit is used to extract the I and Q components from QPSK modulated data.

DC Loop Gain element **408** is the first gain stage of the DC Offset Correction Loop **210**, which multiplies the input receive signal by the value of the spectral inversion bit. The multiplied output produces the I and Q
 30 components of the received signal.

Gain stage element **410** is the second gain stage of DC Offset Correction Loop **210**. Gain stage element **410** multiplies the received signal by a DC Loop

gain value. The DC Loop gain value varies depending on parameters of the CDMA hardware. Gain values vary in accordance with internal number representations of hardware components. The range of numbers represented within a component is determined by the number bits allocated to represent the value. For example, the range of a component 4 bit number may be -7 to 7, while the range of an 8 bit microprocessor would be -128 to 128. If the range of the component values does not match the range of wireless phone controlling microprocessor devices, the values are scaled up or down in order to use the full value range of the controlling microprocessor, so that information is not lost.

Summer element **412** sums the multiplied I/Q sample with previous samples, every 20 milliseconds. Element **412** produces a 9 bit value for input to Pulse Density Modulator (PDM) element **414**.

PDM **414** converts the offset corrected digital signal to analog for use by other CDMA hardware not involved in random number generation.

In the exemplary embodiment, DC Offset Correction Loop is used for the generation one bit of random data every 20 milliseconds, by extracting the least significant bit (LSB) of the summed value produced by summer **412**. The LSB of the 9 bit sum is truly random, as when quantized, it takes on the instantaneous variations of the DC offset component of the input signal.

The random bits generated by the DC Offset Correction Loop are fed to the Random Number Selector Subsystem **214**.

FIG. 5 illustrates the apparatus employed by the exemplary embodiment of the present invention to generate 1 random bit of data from the demodulated digital receive signal input to the Time Tracking Loop **212** every 20 milliseconds. The Time Tracking **212** loop functions to track variations in the receive signal propagation delay over time. The propagation delay in a received CDMA signal is not the same for every bit, and varies randomly.

To track the randomly varying propagation delays, the Time Tracking loop receives each I/Q sample received and advances it by one half chip to produce the early I/Q sample **501**, while delaying it by one half chip to produce the late sample **503**.

The early samples (502-504) and late samples (506-508) are squared in multipliers 502, 504, 506, 508. The squared early I and Q samples are added in summer 510 to produce the energy in the early sample. The squared late I and Q samples are added in summer 512 to produce the energy in the late sample.

5 Subtractor 514 provides the energy difference of the early and late samples to scaling element 516.

Scaling element 516 scales the energy value difference to produce a time tracking phase value. In the exemplary embodiment, the time tracking phase value is a 16 bit number. It can be shown that the LSB bits of the phase value is
10 mathematically random because it is derived from the mathematically random propagation delay inherent in the received signal.

The random bits generated by the Time Tracking Loop are fed to the Random Number Selector Subsystem 214.

Although the present invention is described in the context of generating
15 continuous mathematically random data by using the receive AGC circuit, DC Offset loop, and Time Tracking Loop to exploit random characteristics of CDMA signals, one skilled in the art will understand that the teachings of the present invention are readily extended to other wireless communications hardware and signal characteristics such as frequency tracking loops, searcher
20 processes, thermal noise etc.

The previous description of the preferred embodiments is provided to enable any person skilled in the art to make or use the present invention. The various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to
25 other embodiments without the use of the inventive faculty. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

WHAT IS CLAIMED IS:

1. A method for generating random data bits in wireless
2 communications device, comprising the steps of:
processing a received signal; and
4 extracting said random data bits from said processed receive signal.

2. The method of Claim 1 wherein said step of processing said
2 received signal comprises the step of processing said received signal with a
receive automatic gain control circuit.

3. The method of Claim 1 wherein said step of processing said
2 received signal comprises the step of processing received signal with a DC
Offset Correction Loop.

4. The method of Claim 1 wherein said step of processing said
2 received signal comprises the step of processing received signals with a Time
Tracking Loop.

5. An encryption system, comprising:
2 a random number selector subsystem for generating random numbers
from data bits generated from existing wireless phone hardware; and
4 an encryptor for encrypting a signal using said random numbers.

6. The encryption system of Claim 5 wherein said existing wireless
2 phone hardware comprises a Receive Automatic Gain Control circuit .

7. The encryption system of Claim 5 wherein said existing wireless
2 phone hardware comprises DC Offset Correction Loop circuit.

[illegible]

In wireless communications, transmission devices require continuous supplies of random data for encryption processes. The invention provides a method for generating a continuous pool of truly random data with hardware that is already available in conventional CDMA phones.

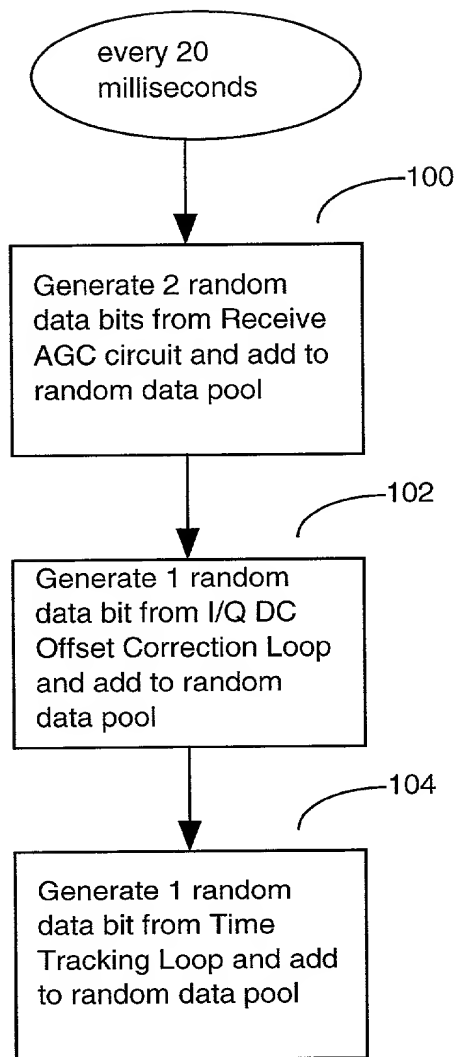


FIGURE 1

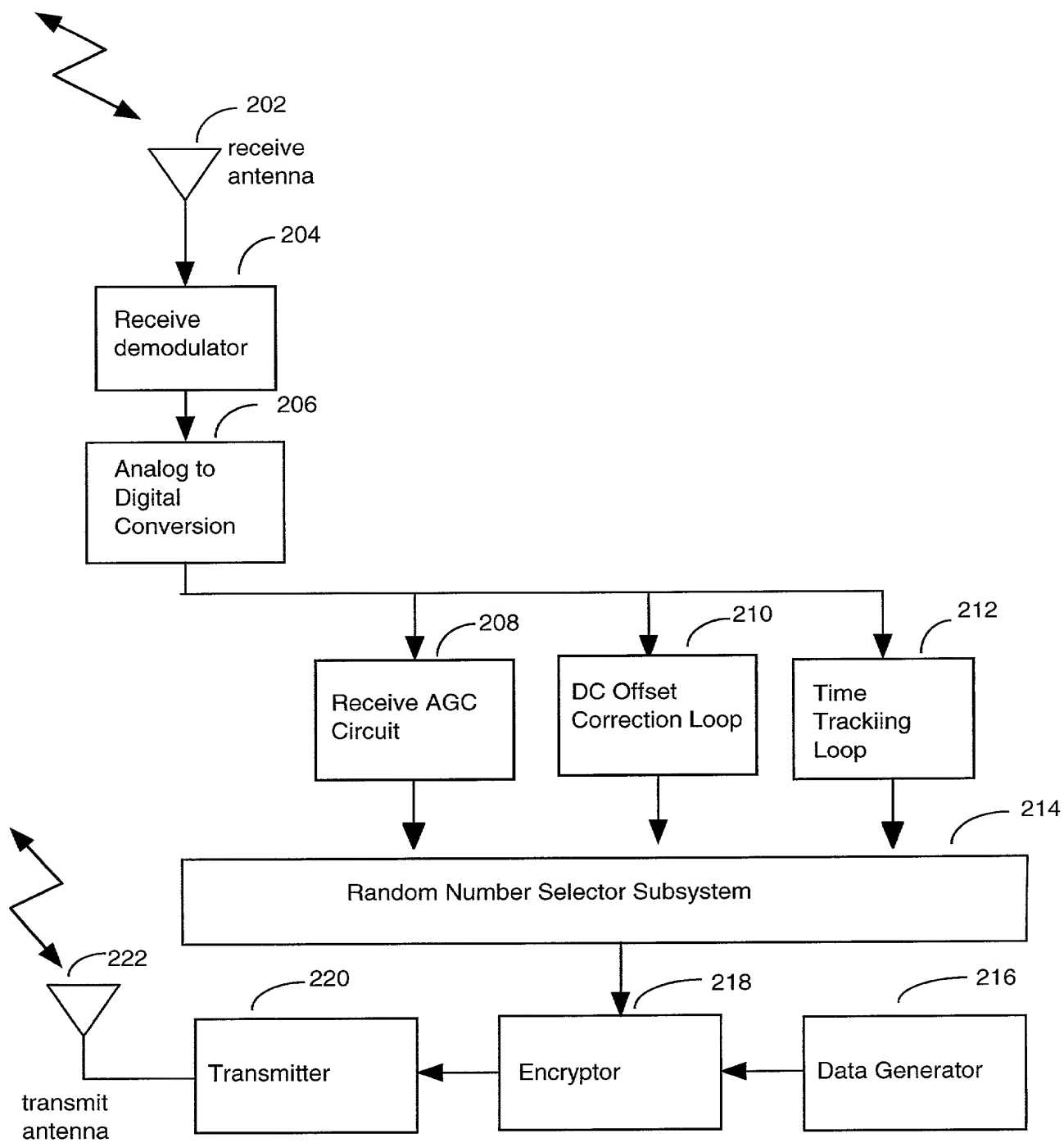


FIGURE 2

FIG. 3 is a block diagram of a receiver system 208, in accordance with an embodiment of the present invention. The receiver system 208 includes a receiver I/Q data block 302, a variable gain amplifier 304, a summer 306, an LNA offset & RX linearizer block 308, and a PDM block 312. The receiver I/Q data block 302 provides input to the variable gain amplifier 304. The variable gain amplifier 304 provides output to the summer 306. The summer 306 provides output to the LNA offset & RX linearizer block 308. The LNA offset & RX linearizer block 308 provides output to the PDM block 312. The PDM block 312 provides output to the RX AGC ADJ block 310. The RX AGC ADJ block 310 provides output to the PDM block 312. The RX AGC ADJ block 310 also provides output to the LNA offset & RX linearizer block 308. The RX AGC ADJ block 310 provides output to the summer 306. The RX AGC ADJ block 310 provides output to the variable gain amplifier 304. The RX AGC ADJ block 310 provides output to the receiver I/Q data block 302. The RX AGC ADJ block 310 provides output to the LNA offset & RX linearizer block 308. The RX AGC ADJ block 310 provides output to the summer 306. The RX AGC ADJ block 310 provides output to the variable gain amplifier 304. The RX AGC ADJ block 310 provides output to the receiver I/Q data block 302.

208

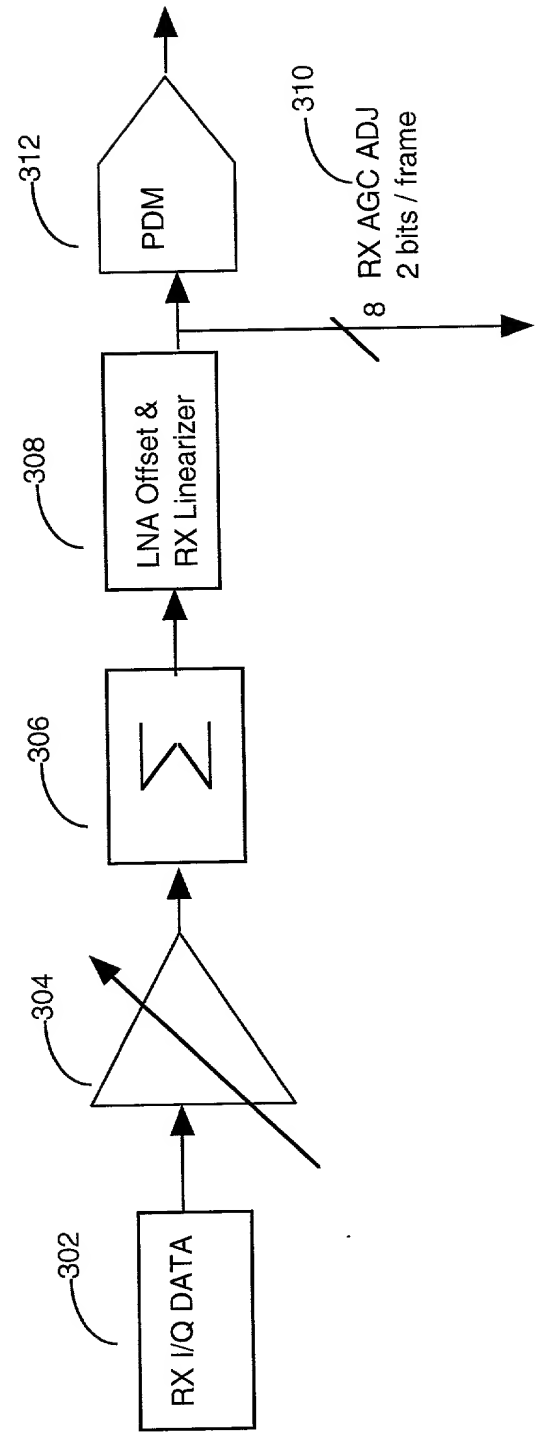


FIGURE 3

210

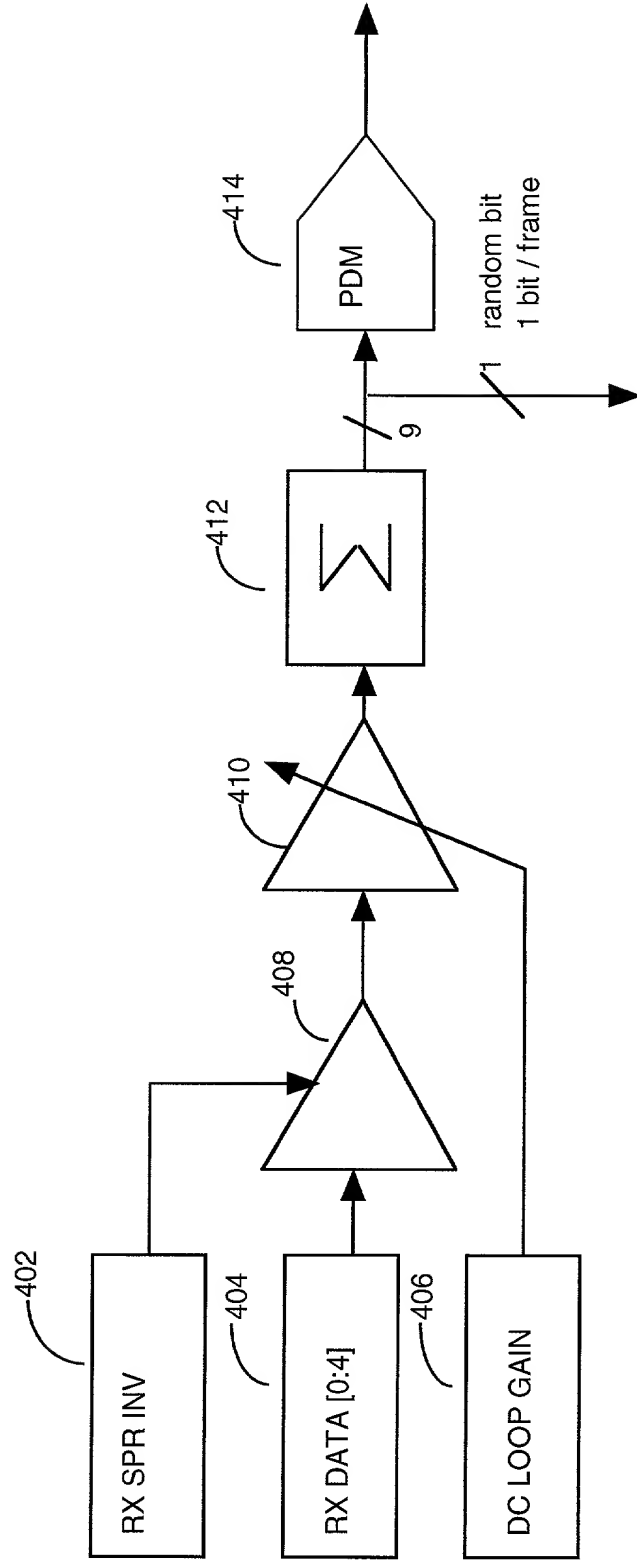


FIGURE 4

212

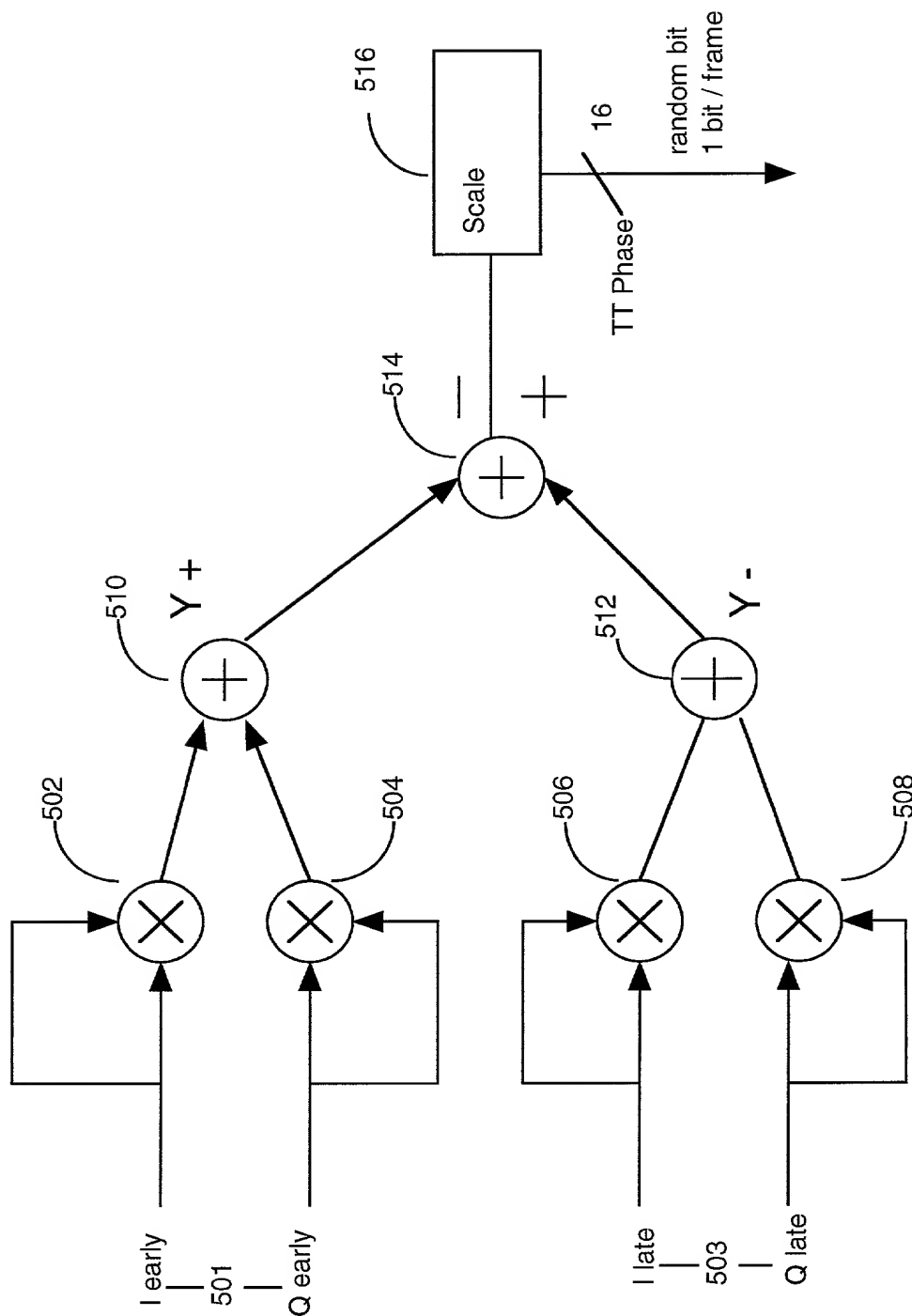


FIGURE 5

COMBINED DECLARATION / POWER OF ATTORNEY

ATTORNEY DOCKET NO.: QCPA990566

AS BELOW NAMED INVENTOR, I HEREBY DECLARE THAT: This Declaration is of the following type:

☒ Original ☐ Supplemental ☐ Continuation-In-Part ☐ Divisional
☐ Continuation ☐ National Stage of PCT

My residence, post office address and citizenship are as stated below next to my name: I believe I am the original, first and sole inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **RANDOM NUMBER GENERATION FOR ENCRYPTING CELLULAR COMMUNICATIONS** the specification of which:

☒ is attached hereto.
☐ was filed on _____ as Serial No. _____
☐ was amended on _____ (if applicable).
☐ was described and claimed in PCT International Application No. _____ filed on _____
and as amended under PCT Article 19
on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, Sec. 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, Sec. 119 of any foreign application(s) for patent or inventor's certificate or of any PCT International application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent or inventor's certificate or any PCT International application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed.

			Priority Claimed	
(Country)	(Application No.)	(Day/Month/Year/Filed)	(Yes)	(No)
_____	_____	_____	_____	_____
(Country)	(Application No.)	(Day/Month/Year/Filed)	(Yes)	(No)

I hereby claim the benefit under Title 35 USC 120 of the United States application(s) listed below, and insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35 USC 112, I acknowledge the duty to disclose material information as defined in Title 37 CFR 1.56(a) which occurred between the filing date of the prior application and the national or PCT International filing date of this application:

(Serial No.)	(Filing Date)	(Status)
_____	_____	_____
(Serial No.)	(Filing Date)	(Status)

I hereby appoint the following attorneys and/or agents to prosecute this application and to transact all business in the U.S. Patent and Trademark Office connected therewith: Russell B. Miller, Reg. No. 31,122, Gregory D. Ogrod, Reg. No. 30,880, Brian S. Edmonston Reg. No. 38,864, Charles D. Brown, Reg. No. 28,285, Thomas R. Rouse, Reg. No. 40,793, Bruce W. Greenhaus, Reg. No. 37,339, Kent Baker Reg. No. 38,822, Tom Streeter Reg. No. 32,007, Thomas M. Thibault, Reg. No. 42,281, Kyong H. Macek, Reg. No. 42,977, Byron Yafuso, Reg. No. P45,244, Roger W. Martin, Reg. No. 39,291, Pavel Kalousek, Reg. No. 44,178 and/or Sean English, Reg. 37,319. Please direct all telephone calls to Russell B. Miller at (858) 658-4833 and address all correspondence to: Russell B. Miller, QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, California 92121-1714.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

COMBINED DECLARATION / POWER OF ATTORNEY

ATTORNEY DOCKET NO.: QCPA990566

Full Name of Sole or First Inventor SANDIP SARKAR	Inventor Signature	Date
Residence 9414 Galvin Avenue, San Diego, California 92126	Citizenship India	
Post Office Address 9414 Galvin Avenue, San Diego, California 92126		

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-4833
Facsimile: (858) 658-2502

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-4833
Facsimile: (858) 658-2502